UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/653,503	09/02/2003	Len L. Mizrah	AIDT 1005-1	3753

22470 7590 03/21/2007
HAYNES BEFFEL & WOLFELD LLP
P O BOX 366
HALF MOON BAY, CA 94019

EXAMINER	
HO, THOMAS M	
ART UNIT	**PAPER NUMBER**
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/21/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/653,503	MIZRAH, LEN L.	
	Examiner	Art Unit	
	Thomas M. Ho	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 September 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *9/22/03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-21 are pending.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 1-21 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

It is uncertain as to what the claims mean when they refer to "An encryption key", "Ephemeral session key", and "Session random key."

Specifically, the Examiner is uncertain as to whether or not these keys are separate keys or references to the same key. To the Examiner's best understanding, Applicant's claims recite a method for producing ephemeral encryption keys. This set of keys includes intermediate ephemeral keys, one of which is selected for encryption. Thus, to the Examiner's understanding, applicant's references to "an encryption key", "ephemeral session key" and "session random key" as recited in the independent claims all refer to the same key. For purposes of examination, the Examiner has interpreted the claims as such.

Claims 7, 14, and 21 are further rejected as being indefinite because they recite the term about 90 seconds. About is a relative term and it is unclear what constitutes about 90 seconds without further context.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-4, 6, 8-11, 13, 15-18, 20 rejected under 35 U.S.C. 102(b) as being anticipated by Perlman, US patent 6363480.

In reference to claim 1:

Perlman discloses a method for producing ephemeral encryption keys at a first station for use in a communication session with a second station, comprising:

- Assigning an ephemeral session key in said first station, in response to a request received by said first station during a session random key initiation interval for use in a first exchange of said plurality of exchanges, where the ephemeral key pairs are announced

for usage in a key initiation interval (Column 5, lines 55-67) , where the interval is the period of time that the ephemeral keys will last. (Column 5, lines 5-25)

- Associating, in said first station, a set of ephemeral intermediate data random keys with said request for use in said plurality of exchanges, where the ephemeral keys are announced as a list including other intermediary ephemeral key pairs. (Column 5, lines 55-67) & (Figure 1)
- Sending at least one message carrying said session key to the second station, and receiving a response from the second station including a shared parameter, which is shared between the first station and the second station, or between the first station and a user at the second station, encrypted using said session random key verifying receipt of the session random key, where the ephemeral symmetric key is sent from first party to the second party (Column 6, lines 1-20), and where the second party sends a response with the symmetric key or "shared parameter" encrypted using a session random key. (Column 6, lines 20-35),
- Sending, after verifying receipt of the session random key at the second station, at least one message carrying an encrypted version of one of said set of ephemeral intermediate data random keys encrypted to be accepted as an encryption key for the session, where upon receipt of the session key at the second party, a message is sent to the first party carrying a message with the encrypted symmetric key which may serve as an encryption key. (Column 6, lines 1-35)

In reference to claim 2:

Perlman (Column 2, lines 45 – 67) discloses the method of claim 1, including assigning said session random key to all communication sessions initiated with the first session, during said session random key initiation interval, where the session random keys are the ephemeral keys used for communications between the first and second parties.

In reference to claim 3:

Perlman discloses the method of claim 1, including assigning said session random key to all communication sessions initiated with the first station during said session random key initiation interval, and associating a different set of ephemeral intermediate data random keys with each communication session, where the first party announces a set of ephemeral key pairs (Column 5, lines 55-67) and each time the second party desires to launch a communication session with the first party, a key is selected from the list, and the first party passes the key to the second party. (Column 6, lines 1-20)

In reference to claim 4:

Perlman discloses the method of claim 1, including

- Providing a buffer at the first station; (Column 6, lines 35-57)
- Storing said ephemeral session random key in the buffer; (Column 5, lines 55- 67 & Column 6, lines 35-57)
- Associating respective session random key initiation intervals with said ephemeral session random keys stored in said buffer. (Column 5, lines 55 – Column 6, lines 20)

- Using ephemeral session random keys from said buffer as session random keys in response to requests received by said first station during said respective session random key initiation intervals. (Column 5, lines 55 – Column 6, lines 20)
- Removing ephemeral session random keys from said buffer after expiry of the respective session random key lifetime in the buffer. (Column 6, lines 35- 57)

In reference to claim 6:

Perlman discloses the method of claim 4, wherein a session random key lifetime in the buffer for said plurality of exchanges has a value within which the plurality of exchanges can be completed in expected circumstances, and said ephemeral session random keys are removed from said buffer after a multiple M times said value of session random key lifetime to engage into establishing a communication session, wherein M is less than or equal to 10, where the ephemeral keys expire for the multiple where M is 1, and the keys expire when their expiration period passes. (Column 6, lines 35-67)

Claims 8, 15 are substantially similar in content to claim 1 and are rejected for the same reasons.

Claims 9, 16 are substantially similar in content to claim 2 and are rejected for the same reasons.

Claims 10, 17 are substantially similar in content to claim 3 and are rejected for the same reasons.

Claims 11, 18 are substantially similar in content to claim 4 and are rejected for the same reasons.

Claims 13, 20 are substantially similar in content to claim 6 and are rejected for the same reasons.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 5, 7, 12, 14, 19, 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman.

In reference to claim 5:

Perlman fails to disclose the method of claim 4, wherein said buffer is managed as a circular buffer.

Perlman discloses that they keys are stored in memory. (Column 6, lines 35-67)

The Examiner takes official notice that managing a buffer as a circular buffer was well known to those of ordinary skill in the art at the time of invention. A circular buffer is a method of accessing memory wherein the reader and writer moves through writing in a block of memory and advances with each read and/or write operation. It is frequently used in situations where data is taken and processed like a queue, or in the case of Perlman, a list of ephemeral keys.

Circular buffer

From Wikipedia, the free encyclopedia

Jump to: navigation, search

A circular buffer is a method of using memory within a computer program.

While the term "circular" is figurative, it alludes to the rotation through the buffer of the positions where the next data will be read and written. When moving through the buffer, the writer moves forward one step each time it writes, and when it passes the end of the buffer it starts again at the beginning. The reader moves through the buffer in the same way. As long as the reader is as fast as or faster than the writer (which is usually the case), the buffer acts as a queue of the next data to be processed. If the writer is faster than the reader, the buffer can fill up.

The term ring buffer is also often used to describe a circular buffer; this term is somewhat more common in multimedia development and informal discussion.

It would have been obvious to one of ordinary skill in the art at the time of invention to use a circular buffer to store the ephemeral keys in order to conserve on the maximum size of the allocated memory necessary to process the list of ephemeral keys.

In reference to claim 7:

Perlman (Column 6, lines 35-67) discloses the method of claim 4, wherein a session random key lifetime in the buffer for said plurality of exchanges has a value within which the plurality of exchanges can be completed in expected circumstances, and said ephemeral session random keys are removed from said buffer after a multiple M times said value,

Perlman fails to disclose expiring the key wherein the session random key lifetime to engage into establishing a communication session is less than about 90 seconds.

However, Perlman discloses that session random key lifetime expires for a period of time. The Examiner takes official notice that establishing a communication session less than about 90 seconds is was well known at the time of invention. For example, website access, or HTTP communication between a client and a server commonly takes less than 90 seconds. During this time, an ephemeral key used to encrypt such communications would also need to be expired in the same period.

Although not explicitly stated, one of ordinary skill in the art would understand that establishing a key lifetime to engage in establishing a communication session being less than 90 seconds would be an acceptable expiration time for a key.

It would have been obvious to one of ordinary skill in the art to expire the key wherein the session random key lifetime to engage into establishing a communication session is less than

about 90 seconds in order to provide ephemeral key communication exchanges for short durations.

Claims 12, 19 are substantially similar in content to claim 5 and are rejected for the same reasons.

Claims 14, 21 are substantially similar in content to claim 7 and are rejected for the same reasons.

Conclusion

8. The following art not relied upon is made of record:

- US patent 6311270 discloses a method of using and creating a random ephemeral key.
- US patent 6490352 discloses an ephemeral key system in the context of an elliptic curve cryptographic paradigm.

9. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on **(571)272-3799.**

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist	Telephone: 571-272-2100	Fax: 571-273-8300
Customer Service Representative	Telephone: 571-272-2100	Fax: 571-273-8300

TMH

March 16th, 2007

Thomas Ho

Benjamin E. Lanier
Examiner AU 2132.